

<b>POLICY AND PROCEDURE</b>	
<b>Policy # and Title:</b> Use of Member Protected Health Information (PHI), Personal Identifiable Information (PII), and Confidential Information	
<b>Primary Policy owner:</b> Compliance	<b>POLICY #:</b> HPA34
<b>Impacted/Secondary policy owner:</b> Select the department(s) that are responsible for compliance with all, or a portion of the policy or procedure as outlined	
1) <input checked="" type="checkbox"/> All Departments 2) <input type="checkbox"/> Accounting & Finance (FIN) 3) <input type="checkbox"/> Administration (ADM) 4) <input type="checkbox"/> Care Management (CM) 5) <input type="checkbox"/> Claims (CLMS) 6) <input type="checkbox"/> Community Marketplace & Member Engagement (MAR) 7) <input type="checkbox"/> Compliance (CMP and HPA) 8) <input type="checkbox"/> Configuration (CFG) 9) <input type="checkbox"/> Cultural & Linguistics (CL) 10) <input type="checkbox"/> Customer Service (CS)	11) <input type="checkbox"/> Facilities (FAC) 12) <input type="checkbox"/> HEDIS/NCQA (QI) 13) <input type="checkbox"/> Human Resources 14) <input type="checkbox"/> Information Technology / Core Systems (IT) 15) <input type="checkbox"/> Pharmacy (PH) 16) <input type="checkbox"/> Project Management Office 17) <input type="checkbox"/> Provider Contracting (CONT) 18) <input type="checkbox"/> Provider Services (PS) 19) <input type="checkbox"/> Quality Management (QI) 20) <input type="checkbox"/> Utilization Management/ BH (UM)
<b>PRODUCT TYPE:</b> <input checked="" type="checkbox"/> Medi-Cal	<b>Supersedes Policy Number:</b> HPA06, HPA35

**I. PURPOSE**

To outline the use of minimum necessary member PHI, PII, or confidential information to accomplish the intended purpose of the use, when full disclosure is not required to complete the request, in accordance with HIPAA accordance with the Health Insurance Portability and Accountability Act (HIPAA), the Confidentiality of Medical Information Act (CMIA).

## II. POLICY

- A. Health Plan of San Joaquin and Mountain Valley Health Plan (“Health Plan”) Workforce makes every reasonable effort to control unauthorized access to, and to only request, disclose, or use the minimum necessary data to complete health care operations, or to carry out any request for member health-related information related to those activities which are for purposes directly connected with the treatment, payment, and health care operations.
- B. The Health Plan Workforce does not divulge the Medi-Cal status (including but not limited to member’s name, date of birth, health services, etc.) of a member without the prior written approval of the member, authorized representative, or the Department of Health Care Services (DHCS), except for treatment, payment, and health care operations.
- C. The Health Plan does not use or disclose PHI without an authorization for the following:
1. Psychotherapy notes
  2. Marketing purposes
  3. Sale of PHI when the Health Plan directly or indirectly receives payment.<sup>1</sup>
- D. The Health Plan prohibits the Workforce from releasing medical information to a person or entity regarding a member receiving gender-affirming health care or mental health care.<sup>2</sup> Additionally, this also prohibits the Health Plan staff from releasing information if a civil action or a foreign subpoena is received regarding a member receiving gender-affirming health care or mental health care.
- E. The Health Plan prohibits the Workforce from using member PHI for any purpose other than arranging for healthcare services.
- F. Minimum Necessary applies to all PHI, PII, and confidential information that The Health Plan receives or creates.

---

<sup>1</sup> 45 C.F.R. §164.508

<sup>2</sup> Civil Code §56.109; Code of Civil Procedure §3421, 3424, 3427, and 3428; Family Code §3453.5; Family Code §3453.5

- G. The Health Plan may rely upon requests as being the minimum necessary protected health information from:
1. A public official or agency who states that the information requested for a purpose permitted under a Workforce member or Business Associate of the Health Plan, and the Institutional Review Board (IRB), or Privacy Board.<sup>3</sup>
- H. The Health Plan discloses PHI, PII, or confidential information without a member's consent, and where minimum necessary does not apply, under the following circumstances:
1. For treatment, payment, and healthcare operations (TPO) purposes except the exceptions listed under section II.C-D.
  2. To the Department of Health and Human Services (HHS), when disclosure of information is required under the Privacy Rule for enforcement purposes.
  3. Uses or disclosures that are required for compliance with HIPAA regulatory requirements.
  4. Other Uses or disclosures that are required by law such as:
    - a. Public health activities.
    - b. Disclosures about victims of abuse, neglect, or domestic violence.
    - c. Judicial and administrative proceedings.
    - d. Law enforcement purposes.
    - e. Specialized government functions.
    - f. Health oversight activities.
    - g. Workers' compensation.
- I. HIPAA exempts certain disclosures from the minimum necessary standard for certain activities, including those that permit a member to exercise the right to access their own PHI.

---

<sup>3</sup> 45 CFR 164.512

- J. The Health Plan complies with HIPAA requirements to de-identify data, which is defined as health information to which there is no reasonable basis to believe that the information can be used to identify an individual. <sup>4</sup> The following are examples of identifiers that are removed to comply with HIPAA: names, all geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, telephone numbers, fax numbers, electronic mail addresses, social security numbers, medical record numbers, and account numbers. <sup>5</sup> When The Health Plan receives any requests for de-identification, the PIU Team ensures it is completed.
- K. Member consent is documented in the Member's Record and made available to DHCS upon request.
- L. The strictest laws that provide additional and/or stricter privacy protections to certain types of PHI, PII, or confidential information are applied by The Health Plan, specifically in areas such as alcohol and drug abuse patient records. <sup>6</sup>
- M. The Chief Compliance Officer (CCO) and Privacy Officer are responsible for ensuring that non-routine uses of PHI, PII, or confidential information including sensitive services, are permissible and necessary. The Health Plan licensed health care personnel are aware of activities in which they are permitted under HIPAA to use PHI without permission from the member.
- N. The Health Plan Contractors, Subcontractors, Downstream Contractors, Network Providers, including Business Associates, (collectively known as "Third Parties") are required to comply with this policy, DHCS regulations, including but not limited to, applicable state and federal laws per contractual agreement, and make PHI available. <sup>7</sup>
- O. The Health Plan Third Parties make PHI available for amendment and incorporate any amendments to protected health information. <sup>8</sup>

---

<sup>4</sup> 45 CFR §164.514(a)

<sup>5</sup> 45 CFR §164.514(b)(2)

<sup>6</sup> Welfare and Institutions code section 5328, California Health and Safety code section 11845.5, and the Information Practices Act

<sup>7</sup> 45 CFR section 164.526

<sup>8</sup> 45 CFR section 164.526

- P. Knowledge of a violation of this policy is reported to the Compliance Department either in person, via email, or anonymously.<sup>9</sup>
- Q. The CCO reviews this policy annually and revises it as necessary.

### III. PROCEDURE

- A. Granting role-based access to member PHI/ePHI to The Health Plan Workforce is established in accordance with policy IT402. The determination of the extent of an employee's access to PHI/ePHI is determined by the employee's immediate supervisor and the Security Officer, consult with the Privacy Officer as needed, and is role-based per policy IT402:
  - 1. Electronic and written access – The Health Plan Workforce is permitted to access member PHI in an electronic and/or written format as necessary to perform their duties.
  - 2. Oral communication – The Health Plan Workforce is permitted to participate in discussions, meetings, hearings, and etc. regarding a specific member's PHI only in circumstances where the Workforce member has information relevant to the communication.
- B. Minimum necessary does not apply to the use of PHI, PII, or confidential information in the following instances:
  - 1. To prepare an accounting of disclosures.
  - 2. Pursuant to a member authorization.
  - 3. Required by law for certain judicial and administrative proceedings.
  - 4. As required for compliance with the HIPAA Privacy Rule.
    - a. Examples include:
      - i. Involvement of staff who are licensed health care professionals to review a member's request to access their PHI, PII, or confidential information.
      - ii. Involvement of the Compliance Department to ensure appropriate application and interpretation of the HIPAA Privacy Rule.

---

<sup>9</sup> Policy CMP01 Response and Prevention of Compliance Violations

C. The Health Plan follows the stricter privacy protections for certain types of PHI, PII, or confidential information such as:

1. Confidentiality of alcohol and drug abuse patient records.
  - a. Records of the identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with the performance of any drug abuse prevention function conducted, regulated, or directly or indirectly assisted by any department or agency of the United State shall, except as provided in subsection (E) of 42 CFR part 2, be confidential and be disclosed only for the purposes and under the circumstances expressly authorized under subsection (B) of 42 CFR part 2.
2. Welfare and Institution Code Section 5328
  - a. Information and records are disclosed only in any of the following cases: in communications between qualified professional persons in the provision of services or appropriate referrals, or in the course of conservatorship proceedings.
3. Information Practices Act
  - a. This law applies to state government, and it expands upon the constitutional guarantee of privacy by providing limits on the collection, management, and dissemination of personal information by state agencies.

D. Protocols for non-routine uses:

1. Uses for purposes not identified in Procedure, section III.A are considered non-routine. Such uses are only made with permission by the Privacy Officer. The Privacy Officer or designee inquires about the following before granting permission for the non-routine uses:
  - a. Is the PHI requested minimally necessary?
  - b. Can data identifying sensitive services be omitted?
  - c. Can a limited data set or de-identified data be used to accomplish the purpose of the request?
  - d. Was a Restriction to Access PHI granted to the member restricting the Health Plan's use of their PHI? If so, permission is denied.

- e. Non-routine uses of PHI in electronic form that require access to the Health Plan systems are documented in an IT Incident by the Compliance Department and include a reason for the use and a termination date when access rights cease.
  - f. Non-routine uses of PHI on portable devices ends as soon as the Workforce member no longer requires the PHI. The Workforce member returns the paper or portable device to the IT Department for destruction.
  - g. Genetic characteristics – The Health Plan does not use or disclose genetic information for underwriting purposes.
- E. The Health Plan controls unauthorized access to PHI, PII, or confidential information in paper form as follows:
- 1. The Health Plan employees are prohibited from leaving PHI, PII, or confidential information in paper form unattended at any time unless it is locked in a file cabinet, file room, desk, or office. Unattended means that the information is not under observation by an employee authorized to access such information.
  - 2. The Health Plan employees is required to dispose of PHI, PII, or confidential information through a Business Associate by shredding or destroying it.
  - 3. The Health Plan Workforce is not permitted to remove PHI, PII, or confidential information from the Health Plan premises, except for routine business purposes, or with the express written permission of DHCS.
  - 4. The Health Plan sends and receives faxes securely through RightFax; however, if a Workforce member should receive or send a fax to an unintended recipient containing PHI, PII, or confidential information, they follow the protocol in HPA07 Reporting Suspected Security Incidents and Breaches.

5. The Health Plan has multi-function printers (MFPs) at both of its facilities, where in order for a Workforce member to print a job, they need to input a PIN number and scan their badge; therefore, there should not be cases where any print or copied jobs containing PHI, PII, or confidential information are left unattended. However, in the case that a Workforce member finds unattended PHI, PII, or confidential information, The Health Plan employee is required to immediately dispose of the document(s) in a secured shred bin.

#### IV. ATTACHMENT(S)

- A. DHCS Medi-Cal Managed Care Plans Definitions (Exhibit A, Attachment I, 1.0 Definitions)
- B. [Glossary of Terms Link](#)
- C. Medi-Cal Managed Care Contract Acronyms List (Exhibit A, Attachment I, 2.0 Acronyms)

#### V. REFERENCES

- A. 45 CFR Parts §160, §162 and §164 HIPAA Regulation
- B. 45 CFR §164.520 Notice of privacy practices (NPP)
- C. California Civil Code §56 - §56.37 Confidentiality of Medical Information Act
- D. California Civil Code §1798.29
- E. California Health and Safety Code (HSC) § 123100
- F. California Knox-Keene Health Care Service Plan Act & Regulations (KKA) §1364.5
- G. California Welfare & Institutions Code (WIC) §14100.2
- H. DHCS Medi-Cal Managed Care Plan Contract Exhibit G. – Health Insurance Portability and Accountability Act
- I. Health Information Technology for Economic and Clinical Health Act (HITECH Act)
- J. The Health Plan Business Associate Agreement
- K. The Health Plan Policy: CMP01 Response and Prevention of Compliance Violations
- L. The Health Plan Policy: CMP02 Records Management and Retention



- M. The Health Plan Policy: HPA05 Business Associate Agreement
- N. The Health Plan Policy: HPA21 Member Rights to Confidentiality of Information
- O. The Health Plan Policy: IT402 Information Systems Access Management

**VI. REVISION HISTORY**

<b>Version*</b>	<b>Revision Summary</b>	<b>Date</b>
001	Added language to policy to ensure compliance with SB 107 per DMHC APL 22-031. See Policy items II.C.	2/17/2023
002	Updated policy language in line with DHCS Exhibit E.1.23 Removed desk level procedure language, included reference to active/related policies.	3/17/2023
003	Included information about process of de-identifying member protected health information (PHI) when full disclosure is not required to complete the purpose of the request in accordance with HIPAA.	6/26/23
004	Included DHCS APL 23-007 Telehealth Services language.	7/14/2023
005	Per Clearwater audit, added language for 45 CFR Parts § 164.500 HIPAA Regulations – permitted uses and disclosures with and without member authorizations.	7/21/2023
006	Per 2024 DHCS Contract, added language about the stricter privacy protections for certain types of PHI.	7/24/2023
<b>Initial Effective Date:</b> 2/17/2023		

**VII. COMMITTEE REVIEW AND APPROVAL**

<b>Committee Name</b>	<b>Version</b>	<b>Date</b>
Compliance Committee	006	2/15/2024
<ul style="list-style-type: none"> <li>• Privacy &amp; Security Oversight</li> </ul>	002	5/12/2023

Committee (PSOC)		
• Program Integrity Committee		
• Audits & Oversight Committee		
• Policy Review	006	12/20/2023
Quality and Utilization Management		
• Quality Oversight		
• Grievance		

### VIII. REGULATORY AGENCY APPROVALS

Department	Reviewer	Version	Date
Department of Healthcare services (DHCS)	DHCS Contract Manager	006	11/2/2023
Department of Managed Care (DMHC)	DMHC Attorney	006	12/5/2023

### IX. APPROVAL SIGNATURE\*

Signature	Name Title	Date
	PRC Chairperson	
	Policy Owner	
	Department Executive	
	Chief Executive Officer	

\*Signatures are on file, will not be on the published copy